INDIANA DATA BREACH NOTIFICATION FORM

OAG Form 1079 (R1 / 09-14)
Identity Theft Unit

OFFICE OF ATTORNEY GENERAL
Consumer Protection Division
Government Center South, 5th floor
302 W. Washington Street
Indianapolis, IN 46204
(317) 233-4393 – Fax

Name and Address of Entity or Person that owns or licenses the data subject to the breach

Name			
Barnes & Thornburg LLP			
Street Address	**City**	**State**	**Zip Code**
11 South Meridian Street	Indianapolis	Indiana	46204
Submitted by	**Title**	**Dated**	
Aaron Lancaster	Counsel	6/29/18	
Firm Name and Address (*if different than entity*)		**Telephone**	
Baker & Hostetler LLP, 1050 Connecticut Avenue, NW, Washington, DC 20036		202.861.1501	
Email	**Relationship to Entity whose information was compromised**		
alancaster@bakerlaw.com	Outside Counsel		

Type of Organization (*please select one*)

- ☐ State of Indiana Government Agency
- ☐ Other Government Entity
- ☐ Educational
- ☐ Health Care
- ☐ Financial Services
- ☑ Other Commercial
- ☐ Not-For-Profit
- ☐ Other – please specify

Number of Persons Affected	
Total (*Indiana Included*)	3
Indiana Residents Only	2

Dates		
Date Breach Occurred (*include start/end dates if known*)	4/20/18	4/23/18
Date Breach Discovered	5/11/18	
Date Consumers Notified	6/29/18	

Reason for delay, if any, in sending notification

Notice is being made to individuals as soon as possible after Barnes & Thornburg learned that personal information may have been accessed by an unauthorized individual and conducted a review to identify which individuals may have been impacted.

Description of Breach (*select all that apply*)

- ☐ Inadvertent disclosure
- ☐ Insider wrong-doing
- ☐ Loss or theft of device or media (e.g. computer, laptop, external hard drive, thumb drive, CD, tape)
- ☑ External system breach (e.g. hacking)
- ☐ Other

Information Acquired (*select all that apply*)

- ☑ Social Security Number
- ☐ Name in combination with (*select all that apply*)
  - ☐ Driver's License Number
  - ☐ State Identification Number
  - ☐ Credit Card or Financial Account Information
  - ☐ Debit Card Number (*in combination with security code, access code, password or PIN for account*)

List dates of previous breach notifications (*within last 12 months*)

NONE		

Manner of Notification to Affected Persons

Attach a copy of a sample notification letter

- [x] Written
- [ ] Electronic (email)
- [ ] Telephone

Identity Theft Protection Service Offered

[x] Yes	Duration	12 months
[ ] No	Provider	Experian Identity Works Credit 3B

Brief Description of Service:
Credit monitoring and identity protection service

Since this breach, we have taken the following steps to ensure it does not reoccur (*attach additional pages if necessary*)

To help prevent something like this from happening in the future, Barnes & Thornburg has removed remote web access for our personnel and is redoubling its ongoing efforts to educate and train employees on how to recognize phishing emails. Remote web mail access is currently being reevaluated for redeployment with multi-factor authentication.

Any other information that may be relevant to the Office of Attorney General in reviewing this incident (*attach additional pages if necessary*)

On April 20, 2018, Barnes & Thornburg detected unusual activity in certain users' email accounts. Barnes & Thornburg immediately secured its email system and began an investigation with the assistance of a leading computer forensic firm.

On May 11, 2018, the computer forensic firm investigating the incident informed Barnes & Thornburg that an unauthorized individual accessed certain emails. Further investigation confirmed the narrow scope of such access. Barnes & Thornburg conducted a thorough review of the material that was accessed and determined, on June 14, 2018, that it included a message that contained two Indiana residents' names and Social Security numbers.

Today, Barnes & Thornburg is notifying the two Indiana residents via U.S. mail in accordance with Ind. Code § 24-4.9 in substantially the same form as the enclosed letter. Barnes & Thornburg is providing one year of credit monitoring and identity theft protection services and also is recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

SUBMIT